

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
<div style="position: relative; height: 100px;"> <div style="position: absolute; top: 0; left: 0; right: 0; bottom: 0; background: linear-gradient(to right, transparent 49%, #ccc 49% 51%, #ccc 51% 53%, transparent 53%); background-size: 4px 4px; background-position: center;"></div> <div style="position: absolute; top: 0; left: 0; right: 0; bottom: 0; background: linear-gradient(to bottom, transparent 49%, #ccc 49% 51%, #ccc 51% 53%, transparent 53%); background-size: 4px 4px; background-position: center;"></div> </div> <p style="font-size: 2em; opacity: 0.5; transform: rotate(-45deg); position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%);">PLANNING DOCUMENT ONLY</p> <p style="font-size: 0.8em; opacity: 0.5; position: absolute; top: 80%; left: 50%; transform: translate(-50%, -50%);">(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</p>				a. FACILITY CLEARANCE REQUIRED TOP SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)	
X a. PRIME CONTRACT NUMBER TO BE DETERMINED		a. ORIGINAL (Complete date in all cases) Date (YYYYMMDD) 20110111		b. REVISED (Supersedes all previous specs) Revision No. Date (YYYYMMDD)	
b. SUBCONTRACT NUMBER					
X c. SOLICITATION OR OTHER NUMBER N00024-11-R-3121		Due Date (YYYYMMDD)		c. FINAL (Complete Item 5 in all cases) Date (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under (previous contract number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under , retention of the identified classified material is authorized for the period of .					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE "FOR BIDDING PURPOSES ONLY."		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) NOT VALID FOR ACTUAL CONTRACT."	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CO		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Contractor Support Services Task Order (TO) under SEAPORTA-E Indefinite Quantity Contract (IQC). Services encompass corporate operations, research and technology, program management, logistics and engineering and instructional systems support for training systems managed by Naval Air Warfare Center, Training Systems Division (NAWCTSD) Orlando, FL.					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA			X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA			X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION				e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)			X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI			X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER	
f. SPECIAL ACCESS INFORMATION			X	h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION			X	i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION			X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION			X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION		X		i. OTHER (Specify)	
k. OTHER (Specify)			X		

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release.

☐ Direct ☒ Through (Specify)

Commanding Officer
Naval Air Warfare Center
Training Systems Division
12350 Research Parkway
Orlando, FL 32826-3275

PLANNING DOCUMENT ONLY

(Proposed release of information will be coordinated through the NAWCTSD Public Affairs Office and the Contracting Officer's Security Representative [Security Manager]).

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review

* In the case of non-DoD User Agencies, request for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classification effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

- a. All contractor personnel shall comply with the DoD Security Agreement (DD Form 441), as well as the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M.
- b. The contractor shall comply with security procedures in effect at all Government sites visited, and where contract work takes place. Contractor work will take place at contractor's facility and various Government sites.
- c. In the course of this contract, the contractor will require access to documents, which contain critical technology. The contractor needs to store documents to deny access, and destroy them to prevent reconstruction when they are no longer needed. Although UNCLASSIFIED, these documents will have limited distribution statements.
- d. Attachment (1) provides guidance on the proper handling procedures for FOUO material.
- e. Software shall be developed according to NISPOM, par. 8-302 and contract requirements. See attachment (2).
- f. Any classified information generated in the performance of this contract shall be classified according to the markings shown on the source material.
- g. Prime contractor is responsible for issuing DD254s, as required, to subcontractors.
- h. The contractor shall ensure that common sense TEMPEST measures are implemented during all times of classified processing. Such measures include, but are not limited to: (1) no wireless communications equipment in area during classified processing, and (2) physical separation of classified processing system and other equipment, such as a telephone, fax, etc. Attachment (3), TEMPEST Questionnaire, must be completed and forwarded to the address indicated, with a copy to the Security Office of this Contracting Agency, for final evaluation/determination of any additional TEMPEST requirements. When responding to Question 9 of the TEMPEST Questionnaire, include general identification of contractual effort (i.e., COMS for ..., etc), a statement defining/summarizing types of classified data, and level of classified information being processed.

"SEE BLOCK 13, SECURITY GUIDANCE, CONTINUATION PAGE"

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirement to the cognizant security office. Use Item 13 if additional space is needed.) ☐ Yes ☒ No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Used Item 13 if additional space is needed.) ☐ Yes ☒ No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL
Darren Smith

b. TITLE
Contracting Officer's Security
Representative

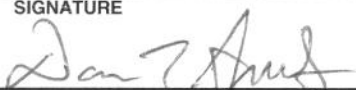
c. TELEPHONE (Include Area Code)
(407) 380-8243

d. ADDRESS (Include Zip Code)
NAVAIRWARCENTRASYS DIV
12350 Research Parkway
Orlando, FL 32826-3275

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATION CONTRACTING OFFICER
☒ f. OTHER AS NECESSARY

e. SIGNATURE



1/11/11

PLANNING DOCUMENT ONLY

DD Form 254, Department of Defense Contract Security Classification Specification
RFP Number N00024-11-R-3121

Item 13, SECURITY GUIDANCE (Continued)

i. The contractor shall develop, implement, and maintain a facility level OPSEC program to protect classified and sensitive unclassified information to be used at the contractor facility during the performance of this contract. The OPSEC requirements may be included in the contractor's Standard Practice Procedures (SPP) or Technology Control Plan (TCP), whichever is more applicable.

j. Contractor will incorporate security procedures to mitigate risks associated with wireless devices in areas where employees are working with classified information and/or where classified discussions may be held. Such countermeasures may range from ensuring wireless devices are turned off or not used in classified areas to, in some cases, not permitting devices in the area.

"FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation by a DoD Agency. It is not authorized as a substitute for a security classification but is used on official government information that may be withheld from the public under Exemptions 2 through 9 of the Freedom of Information Act.

Use of this designation does not mean that the information cannot be released to the public, only that it must be reviewed by the government prior to its release to determine a significant and legitimate purpose is being served by withholding this information or any part(s) of it.

An unclassified document containing FOUO information will be marked "For Official Use Only" (FOUO) at the bottom of the front cover (if any), the first page, each page containing FOUO information, back page, and outside back cover (if any). If a document is classified, and a page contains both classified information and FOUO information, the document will carry the highest classification contained on each page and where a paragraph/portion is only FOUO, that paragraph/portion will be marked as such.

Removal of the FOUO designation can be accomplished only by the originator or other competent authority. This information may be disseminated by contractors to their employees and subcontractors who have a requirement for the information in connection with a contract.

During working hours, FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access such as a locked desk or locked file cabinet. When FOUO information is no longer needed, it may be disposed of by tearing, shredding, etc. which precludes reconstruction.

FOUO information may be transmitted by regular US Postal Service mail or US commercial express mail services authorized for unclassified material. The transmission of FOUO material by regular telephone or electronic mail is discouraged unless absolutely necessary in the performance of the contract and is time sensitive. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, should be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), when practical

FOUO material is not to be placed on Non Government World Wide Web sites or any site that is accessible to the general public. FOUO information may be transmitted over telephone lines in digital form such as fax machines or telecopiers.

The unauthorized disclosure of FOUO information does not constitute a security violation; however, the originator or User Agency will be informed of the disclosure. The unauthorized disclosure of FOUO information that is protected by the Privacy Act may result in the criminal sanctions under that statute.

Additional guidance is available by contacting the User Agency Security Office.

Vendor Integrity Statement for Software

1. DESCRIPTION

The Vendor Integrity Statement for software shall be a written and signed contractor certification that assures that each contractor-developed software item delivered to the Government has been examined according to National Industrial Security Program Operating Manual (NISPOM), paragraph 8.302. In addition, any Government-authorized public domain (Open Source) software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall be subject to the examination and certification described herein and included as part of the VIS when integrated into the trainer. The results of the examinations must indicate that the software has no elements that might be detrimental to the secure operation of the resource operating system. Elements detrimental to the secure operation include:

- a. Malicious code
- b. Trojans, worms, logic bombs, and other computer viruses
- c. Backdoors
- d. Buffer overflows or memory leakage
- e. Ad-ware, Spy-ware, or web bugs that have the ability to track user behavior
- f. Code that permits functions that are beyond the actual publicized intent of application capability
- g. Software that will not function properly with the operating system configured securely

2. BACKGROUND

DoDI 8500.2, Information Assurance (IA) control DCAS-1 requires the acquisition of all IA and IA-enabled Information Technology (IT) products that are Commercial Items (per FAR Part 2.101), be limited to products that have been evaluated or validated through one of the following sources – the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the National IA Partnership (NIAP) Evaluation and Validation Program, or the Federal Information Processing Standards (FIPS) validation program. Paragraph 4.18 of DoD 8500.1 requires that IA-enabled IT products incorporated into Department of Defense (DoD) information systems be configured in accordance with DoD-approved security configuration guidelines.

3. CONTENT AND FORMAT

The Vendor Integrity Statements for trainer application software shall consist of the following certification, dated and signed by an authorized representative of the contractor, on company letterhead:

TO: NAVAIR Orlando

RE: Vendor Integrity Statement for Software for Device XXXXX, under Contract N61339- XX-X-XXXX

I certify that for xxxx software (list all developed and public domain software items or attached a list), version xx, there are no elements that might be detrimental to the secure operation of the resource operating system. The software runs with the operating system configured per contract requirements.

Signed

Company Representative

TEMPEST REQUIREMENTS QUESTIONNAIRE
(FOR CONTRACTOR FACILITIES)

1. This TEMPEST Requirements Questionnaire (TRQ) must be completed and sent to the contracting authority and the Certified TEMPEST Technical Authority (CTTA) within 30 days after contract award for all contracts where National Security Information (NSI) will be processed and the requirements of item 13 of the DD Form 254 have been met.
2. The prime contractor cannot pass TEMPEST requirements to subcontractors. Subcontractors must submit a Contractor TRQ prior to processing.
3. The TRQ is for information collection only. It is not a directive or an implied requirement, nor is it an encouragement to procure TEMPEST equipment or any type of shielding for use on this contract. DO NOT initiate any changes to equipment of facilities for TEMPEST unless it has been recommended by the CTTA and specifically directed by the contracting authority.
4. The contracting authority will not issue any directives concerning TEMPEST until after the contractor submitted TRQ has been evaluated by the CTTA and resulting recommendations received. To fully evaluate the TRQ, the CTTA may request additional information concerning the facility, its physical control, the equipment which will be used to process NSI, etc.
5. The contractor shall ensure compliance with any TEMPEST countermeasure (s) specifically directed in writing by the contracting authority.
6. Please provide the information requested in paragraphs 7 through 20 and return to the contracting authority identified in item 16 of the DD Form 254 and to the CTTA at :

COMMANDING OFFICER
SPAWARSYSCEN
CODE 723
P.O. BOX 190022
NORTH CHARLESTON SC 29419-9022

7. Provide the name, address, position title, and phone number (at the facility where classified processing will occur) of a point of contact who is knowledgeable of the processing requirements, the types of equipment to be used and the physical layout of the facility.
8. Provide the specific geographical location, address, and zip code, where classified processing will be performed.
9. What are the classification level (s) of material to be processed/handled by electronic or electromechanical information system (s) and what percentage is processed at each level?
10. What special categories of classified information are processed?

ATTACHMENT (3)

11. Is there a direct connection (wireline or fiber) to a Radio Frequency (RF) transmitter (s) located either locally or at a remote site?
12. Are there any RF transmitters located within 6 meters of the system processing National Security Information or the system's RED signal lines?
13. Describe how access is controlled to your facility including the building, compound, plant, property, and/or parking lots. Where are visitors first challenged/identified? Include controls such as alarms, guards, patrols, fences, and warning signs. Provide a simple block diagram of the equipment, the facility and the surrounding areas. The diagram (s) should extend out to the nearest uncontrolled area on each side of the facility, such as a military base perimeter, plant property line, commercial building or residential area.
14. Are there other tenants in the building who are not U.S. department/agencies or their agents?
15. Are there any known foreign business or government offices in adjacent buildings?
16. Provide the make and model number of all equipment used to process, transfer or store classified information. Include computers, peripherals, network servers, network hardware, multiplexers, modems, encryption devices (COMSEC), etc.
17. Have on-site TEMPEST tests been conducted on any of these equipment (s)? If so, which ones? When was the test (s) conducted? Who conducted the test (s)? Have all deficiencies (if any) been resolved?
18. Has a TEMPEST Facility Zoning test been conducted? If so, who conducted the testing and when?
19. Is this company foreign-owned or controlled? If so, what is the country?
20. Provide name, code, telephone number, and address of the Contracting Officer's Representative, the contract number and the sponsoring command.